Summary of the proceeding of the
Workshop on Legal Framework for privacy, Data Protection and Security

Civil Services Officers Institute
Kasturba Gandhi Marg
21st July, 2010

Participants

i. **Shri. Shantanu Consul, Secretary (Personnel)**
ii. **Shri. Rajeev Kapoor, JS(AT&A), DoPT**
iii. **Shri. Arun Goyal, Director, Financial Intelligence Unit, D/o Revenue**
iv. **Dr. C. Chandramouli, RGI, MHA**
v. **Shri. Raghu Raman, CEO NATGRID, MHA**
vi. **Shri. Gulshan Rai, Director General, Deptt. of IT**
vii. **Major- General (Dr.) R. Siva Kumar, CEO, NSDI and Head, NRDMS, D/o of Sc. and Tech.**
viii. **Shri. Rahul Matthan, Partner Trilegal**
ix. **Shri. Sunil Abraham, Executive Director, Centre for Internet & Society**
x. **Shri. Deepak Maheshwari, Member, National Commission on IT and Telecom, CII**
xi. **Smt. Anuradha Das Mathur, Founder Director, 9.9 Media Work, Pvt. Ltd**
xii. **Shri. Kamlesh Bajaj, CEO, DSCI**
xiii. **Shri. S.K. Chakrabarti, DDG Office of RGI, MHA**
xiv. **Dr. Shashank Saksena, Director, Deptt. of Finance Services M/o Finance**
xv. **Shri. M.R. Umarji, Chief Legal Adviser, Indian Bank Association**
xvi. **Smt. Zoya Hadke, Dy. Legal Adviser, D/o Legal Affairs**
xvii. **Smt. Arunima Sharma, Dy. Director, CII**
xviii. **Shri. K.G. Verma, Director,DoPT**
xix. **Smt. Anuradha Chagti, DS(RTI),DoPT**
xx. **Shri. R.K. Girdhar, US(RTI),DoPT**
xxi. **Shri. B. Sengupta, DO(IR),DoPT**
xxii. **Shri. Vijay Kumar, SO(IR),DoPT**

1. Director (RTI) welcomed the participants to the workshop.

2. Initiating the discussion Shri Shantanu Consul, Secretary, Department of Personnel & Training, highlighted the need for a comprehensive Privacy Law for India and also detailed

the formation of a group to lay down legal framework for such a legislation. He stated that this workshop has been organized to elicit views of the practitioners in the field and also the civil society organizations regarding proposed legislation. He highlighted that as India is transforming, more digital data processing is being undertaken and issues of privacy have come to the fore. While on one hand the legislation should ensure that personal data about individuals is kept private we will also have to balance the need for sharing of data for legitimate needs including those of national security. Further, on one hand while the framework and legislation will have to be India-centric, on the other because BPO Industry is so vital for India and because cross border data flows will take place, we need to ensure that the proposed legal framework is able to get acceptability by international community. He hoped that the deliberation would help us evaluate various approaches adopted across the world in the area of privacy legislations and to determine the broad features of the legal framework that may be proposed for our country at this stage.

3. Shri Rahul Matthan, Partner Trilegal presented before the participants the results of a study on the international approach to Privacy and data protection. The study was spread over 39 developing countries and 41 developed countries wherein 83% countries had umbrella legislation, 5-6% have sector specific legislation and several countries have no specific legislation. In case of sector legislation, there was fear of overlaps in judicial decision which would have to be kept in mind, in case India went in for a sector specific approach. He differentiated between the concept of personal data and personal sensitive data, which may need to be handled with different degrees of care. Personal data being data that can be used to identify a person, for example as a natural person or a legal person (association, corporation etc.) and person sensitive data would be specific data like educational qualification, race, ethnic origin, which may affect a person's employment chances or any other entitlements. The people involved in this are the data subjects or concerned persons whose data is being used, data controllers, who decide how the data will be used, data processors who process the data and data regulators. It would be very important while framing the legal framework to specifically regulate data collection, processing, data storage, data access, the regulators and the penalties. The legal framework which is laid down needs to be applicable to both the public and the private sectors. Issues of cross border transfer of data have to be addressed as some countries prohibit trans-border transfer of data. Europe prohibits transfer of data to any country which has less stringent laws, except the US where there is a safe harbor mode. Similarly Australia has a regulator to

prosecute offences in respect of data transfer **but it is not applicable to data in transit**. UID is applicable to residents of India, The relation between residents and citizens would need to be defined. India too would need to look into such arrangements.

He emphasized the security concerns in data collection. For example, banks collect data but outsource the processing to outside agencies. The norms in such case have to be defined. At the point of data collection itself, the subject needs to be informed why the data is being collected and explicit consent must be taken every time personal sensitive data is used. The data subject should have the choice of withdrawing his consent at any time. At the moment data is not being secured in this country and it should be ensured that only relevant i.e., accurate and up to date data is being collected. The regulator needs to be notified every time data is collected.

Data processing should be in accordance with the stated purpose and should be processed only after notification. If data is collected for a magazine subscription then it should be used only for that purpose and only that data which is essential for an outsourced processor to know, should be divulged to him. Like the courier company of the magazine may know only the address of the subscriber and not the payment details.

Data storage should be transaction based and should be deleted after use. However in an ongoing transaction, like a magazine subscription the storage of data should in such a way that the data owner/ subject is non – identifiable.

Data security should be maintained by technical and organizational controls. There should not be unauthorized access to data. There should be a record of all people who have access to data. There should be a Chief Data Security Officer in each organization. Data transfer should only be in an encrypted form.

Data access for the data subject has to be provided at all times. He should have information on the purpose for collecting the data and the recipients of such data. The legal framework should not overlook the requirements of the needs of Persons with Disabilities to access data. Regulator will define the compliance laws, exemptions, penalties and the level of privacy required for private to private interaction.

He highlighted the fact that for a country like India, issues like distinctive names and literacy levels would have to be properly addressed. A copy of the presentation is at **Annexure 'A'**.

4. Shri C. Chandramouli, Registrar General of India, informed the participants that the data collected in the Census is confidential as per Census Act 1948. This data is not to be revealed even to the Courts of law. However, since the RTI Act came into being, repeated requests were being made to reveal certain information that pertained to individuals. Each and every time such a request was made, the information was being denied under Section 8(1)(j) of the RTI as it is a third party data that is not to be revealed except with the express consent of the individual who has given such data. So far the Information Commissioners have been accepting this plea. However the RGI wanted that Census and data collected under various surveys like Sample Registration Survey, Annual Health Survey etc should be protected under the RTI Act or Privacy Law itself. This is important because the information given under these various surveys are in the nature of privileged communications which the organisation collecting it is bound to protect. Further, as a matter of policy, sensitive data like religion is not tabulated below certain levels of geographical aggregation in order to protect against any profiling. There is a distinct possibility of demands being made to reveal such data under the RTI. Here it would be difficult to take the plea of third party. This would prove prejudicial to the public good. It would therefore be necessary to exempt such data from the purview of RTI. The RGI pointed out that the proposed legislation should consider effective means of protecting the data collected under the Census and Surveys.

   The National Population Register (NPR) is a flagship programme of the Government which is aimed at creation of a comprehensive Biometric based Identity system in the Country. This envisages collection of 15 fields of individual information of every usual resident of the country in the first instance. This exercise has been completed to a large extent. In the next phase, photograph, 10 fingerprints and 2 Iris prints would be added to this database. The biographic and biometric database would then be subjected to de-duplication by the UIDAI and a unique Identification Number would be generated for every usual resident of the country. Identity (smart) Cards would then be issued to every usual resident. Creation of what is probably the largest database in the world would bring in its wake the need for laws and regulations for data protection and privacy on the one hand while permitting the legitimate use of the database for genuine Government purposes on the other. The RGI is in the process of framing Rules under the Citizenship Act, 1955 for this purpose. The RGI requested that the Committee should take this into consideration while drafting the policy/legislation on privacy. In this context he also referred to the draft bill relating to UID that has been put up for consultation.

It was also pointed out that withdrawal of consent especially in cases like NPR was not possible as it was mandatory to register all citizens/usual residents under the Citizenship Act. As NPR Card would also carry the UID Number, it cannot be said that the UID exercise was a voluntary exercise and that persons can withdraw their consent.

5. Shri Gulshan Rai, Director General, Department of Information Technology presented the provisions of data protection of the IT Act, 2000. The demand for the amendment of the Act arose from the industry. 38% of the BPO industry of the world is in India and deals with massive cross border inflow and outflow of data. The Act was amended two months ago and deals with data security, protection of personal sensitive data and encryption of data. There was still no feed-back on it. There was no distinction between sensitive personal data and just personal data in the IT Act, 2000. It deals only with digital data and is framed like an umbrella legislation. A copy of the presentation is at **Annexure 'B'**.

6. The participants pointed out that the IT Act, 2000 dealt only with digital data and not on data on broader issues. The implementation mechanism needs to be strengthened with a Commission like the Central Information Commission to adjudicate on matters. The Commission should also provide clearances for usage of data. It was stressed that UID should not fail due to inadequate data protection. Some of the participants felt that there was a need for new legislation to be modeled on the U.K. Data Protection Law and aligning sectoral legislation to the umbrella law.

7. Shri Kamlesh Bajaj, CEO, DSCI gave a background to the definition of privacy and the privacy laws since 1890. The main concern in the modern day was how is personal information used or shared; protected and who is accountable? These issues have gained a lot of importance with the coming of internet making data available to all in the real time. This has led to emergence of privacy standards and Codes. ISO and the European standards body CEN are studying the feasibility of an international privacy standard. Different privacy approaches have been followed till now. The EU Data Protection Directive views privacy as a fundamental human right and the government is responsible for providing privacy to citizens. US on the other hand, has a sector specific approach. Privacy there is seen as a commodity subject to the market and is cast in economic terms. The APEC approach is based on the accountability principle, the data protection obligations flow along with the data in trans- border data flows. Privacy codes have been in practice for a long time as part of self regulation, like organizational codes, sectoral codes, functional codes, technological

codes and professional codes. Privacy standards extend the self regulatory code of practice and maybe either voluntary regulation standards or statutory regulation standards.

He highlighted that the changing society had a bearing on privacy issues in India. There was a quantum jump in the use of technological solutions for delivery of financial services, transformation from a joint to a nuclear family, fast climbing individualism, the younger age group of 25-35 years and the emergence of personalized services. Issues like telemarketing calls, increased awareness about personal information being collected, internet connectivity, media coverage need to be considered. There were some sectoral attempts like the ethical guidelines for biomedical research, the do not call registry and the RTI Master circular, 2007 but these were not enough. Cyberspace and cyber crime need to be addressed. There were also issues of privacy and national security. Cyber attacks can support military operations thus effecting the economy of a country. He stressed the fact that privacy laws should be in line with the country's security, keeping in view India geopolitical position. In this context he highlighted the following issues:

- Is privacy a fundamental right?
- Does a citizen voluntarily give his PI to government databases; or there is threat of services being denied to them?
- In India, the debate on having a strong encryption to fulfill business requirements versus mandating level of encryption (by government) that the Law Enforcement Agencies can break for ensuring National Security, is delaying the formulation of a national **Encryption Policy**
- Large databases maintained by different agencies can be **correlated** to create profile of individuals – **information collected for one purpose used for other purposes**. Banks can deny credit on the basis of such correlation; house loans can be denied; medical policies may not be issued based on prior information of diseases, etc., jobs can be denied with information profiling from social networking sites.
- **Biometrics** once collected for unique identification can be used for **tracking criminals**.
- **CCTV monitoring** at public places – so useful in **tracking terrorists** after incidents - **violates privacy**
- Does Privacy create hindrance to data flow or usage, undermining the **economic value of data** ?
- **Wi-Fi** data collection, use of **cookies** to **collect personal information** and analyze personal preferences, use of search keywords for targeted advertisements, **street view**

application that **encroaches personal privacy**, software updates asking for personal data that is used for **cross selling** and **up selling** products and services.

- **Social networking site**, claiming ownership of user data, like Facebook did in 2009, but reverted.
- **Data Retention** – national security regulations asking ISPs, network service providers and intermediaries to retain user traffic information as well as message content – leading to **breach of citizens' privacy**. Countries like Germany ruled out such retention.
- Security scanners particularly '**Full Body Scanner**', that potentially lead to **breach of privacy of an individual.**

He recommended:

- Have light weight regulations based on global privacy principles that value economic benefits of data flow and usage, while guaranteeing privacy to citizens
- Avoid bureaucratic structures that could hinder business interests and lose the spirit during implementation
- Rely on self-regulation of businesses that promote practices, making the privacy program relevant to technology advancements
- Provide legal recognition to the role of self-regulatory bodies, promoted by industry associations, in enforcing privacy codes in the interest of citizens' rights
- Establish a mechanism, in the form of public private partnership, to resolve the disputes and grievances of citizens

A copy of the presentation is at **Annexure 'C'**.

8. Shri M.R. Umarji, Chief Legal Adviser, Indian Bank Association stated that no law was required for the banks as there was enough legal protection available in the existing laws. Obligation of secrecy about the affairs of the customers is an implied term of the contract between Banker and Customer. There is a statutory recognition of the obligation of secrecy. The only exemptions to this were the consent of the account-holder or compulsion of Law.

   Banks had taken adequate measures to protect data like, appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and also against accidental loss, destruction or damage to data, a Preventive Vigilance Manual for Computerised Branches of Banks to ensure secrecy, integrity and timely availability of customer data maintained centrally and accessed through various channels and a Manual on New Controls and Procedures for operations under the Core Banking and Alternate Channels. He however desired that Section 8 of the RTI Act, 2005 should incorporate the

banker's obligation of secrecy and protection. A copy of the presentation is at **Annexure 'D'**.

9. Dr. Shashank Saksena, Director, Deptt. of Finance Services M/o Finance felt that privacy principles have to be implemented in Banking Laws, though there was no need for a separate legislation for banks.

10. Shri Deepak Maheshwari, representing CII, highlighted the issue and challenges in a legal and regulatory framework for privacy, data protection and Security. He stressed that there should be a right balance between individual privacy rights and the need for government to investigate and prosecute criminals and terrorists; storage of data in the landscape of cloud computing; security of data at rest and at transit; the location and routing of data; cross-border jurisdictional issues; and responsibilities of different parties in the event of a data breach. There should be a discussion paper on the core areas of concern, before the legal framework is laid down. A copy of the presentation is at **Annexure 'E'**.

11. Shri. Sunil Abraham, Executive Director, Centre for Internet & Society laid down the main takeaways from the legislations in US and Europe. He felt that an umbrella legislation like the European one was a better approach for India. Secondly, a graduated approach should be adopted from personal data to personal sensitive data. There was a need for a regulator like a Privacy Commissioner to take proactive action and issue guidelines on access to data collected under programmes like JNNURM, NREGS and UID. There should be data collection with the knowledge or cooperation of the data subjects, safeguards for private sector should be built in. Safeguards should be built-in for the private sector considering that the Copyright Law allows for reverse engineering and circumvention of Technological Protection Measures (TPM). There is a need to address old rights in a new world, in the non-digital age, no one checked what is read by an individual in a library, however with the coming in of digital e-book reader like 'kindle' , companies like Amazon have exact data on a persons' reading preferences. There are, thus conflicts between WIPO Treaty for Visually Impaired and the amendment proposed to the Copyright Law. Anonymous and pseudonymous sources should be protected along with whistle blowers. Safeguards need to be built-in in cross border transactions, the technical considerations of data collected under UID so that there is no impersonation of biometric data or tailgating. Data retention principles should lay down what is collected, how much of it is appropriate, how is it stored, till when will it

be valid, with whom will it be shared and under what terms and will there be any breach notification. A copy of the presentation is at **Annexure 'F'**.

12. Ms. Anuradha Das Mathur, Founder Director, 9.9 Media presented the corporate world's perspective on privacy. She informed that privacy issues are being handled on priority in the corporate world and there are a number of chief information security officers, who are sensitized to the issue of privacy. She stressed the fact that though the IT Act was suitable and adequate it is still very vulnerable. Synergy between the sovereign and the corporate needed to be built in and penalties for impinging on privacy should be laid down. However, privacy control should not hamper normal business operations. The legal framework for India should keep in mind that privacy was not a major issue for a large part of India. Corporate India could add value in this field by giving inputs in policy, creating awareness about the concept, engaging proactively with internal and external stakeholders, governance and accountability, managing compliance by building traction and capability across the privacy officer community and providing tools on how to measure the success of the privacy initiative. A copy of the presentation is at **Annexure 'G'**.

13. Shri Rajeev Kapoor, Joint Secretary (AT&A), Department of Personnel & Training, thanked the participants for a meaningful and thought provoking discussion. He highlighted that the broad consensus that is emerging is that we do need an umbrella legislation on the subject which should enable sector-specific guidelines to be framed. He mentioned that framework will have to strike a right balance between the 'Right to Information' and the 'Right to Privacy', between bringing in transparency in government for curbing corruption and making public beneficiary-wise details which may impinge on individuals' privacy, and need for privacy versus need for sharing information such as credit information in banking industry. He also highlighted the fact that in the context of the government adequate attention to privacy issues had not been given while launching several e-governance applications, and this also need to be addressed. He also mentioned that since we have the knowledge and experience of privacy laws across the world we may learn from the best practices and try to incorporate them in the proposed legal framework.

    At the end, he once again thanked all the participants for their contribution and mentioned that the group would be consulting with the stakeholders again before finalizing the proposed framework.